ABSTRACT OF THE DISCLOSURE

One or more methods and systems of generating pseudo-random numbers that are used as encryption keys in cryptographic applications are presented. In one embodiment, a method of generating pseudo-random numbers is performed by sampling output sequences of a linear feedback shift register with a specified periodicity. In one embodiment, the generating of pseudo-random numbers using linear feedback shift registers is accomplished by periodically switching between iterative outputs generated by multiple linear feedback shift registers. In one embodiment, a method of encrypting a pseudo-random number generated by a linear feedback shift register comprises using a nonlinear operator. In one embodiment, a method of further encrypting a pseudo-random number is accomplished by using a hashing function whose initial value varies over time by way of a function operating on one or more variables. In one embodiment, an apparatus for generating pseudo-random numbers using linear feedback shift registers comprises a digital hardware.